The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

08/26/2014

SUBJECT:

Vulnerability in Slider Revolution Responsive plugin for WordPress Could Allow for Arbitrary-File Download

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Slider Revolution Responsive plugin for WordPress CMS which could allow an attacker download arbitrary files. Slider Revolution Responsive is a plugin for WordPress content management application, which allows for image transition effects, an image preloader, video embedding, user interaction, etc. Successful exploitation of this vulnerability may allow an attacker to download arbitrary files from the Web server and obtain potentially sensitive information.

THREAT INTELLIGENCE

At this time, CIS has observed this vulnerability being exploited in the wild. Vulnerabilities have also been observed in other slider plugins, but haven't been observed in the wild.

SYSTEM AFFECTED:

ENVATO Slider Revolution Responsive 4.1.4

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

The Slider Revolution Responsive plugin for WordPress is prone to a vulnerability that lets attackers download arbitrary files through a web browser. Specifically, this issue occurs because it fails to sufficiently verify the file submitted through the 'img' parameter of the 'admin-ajax.php' script.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Slider Revolution Responsive versions immediately after appropriate testing.
- Run all software as a non-privileged user with minimal access rights.
- Update or disable vulnerable Slider Revolution Responsive versions immediately after appropriate testing.
- Consider implementing a web application firewall and/or File Integrity Monitoring solution for greater risk management for web-based applications
- Perform regular web application and vulnerability scans of all public facing equipment. These scans should be performed, at a minimum, quarterly, but ideally on a monthly basis.
- Ensure that systems are hardened with industry-accepted guidelines.
- Keep all operating system, applications and essential software up to date to mitigate potential exploitation by attackers.

REFERENCES:

Code Canyon:

http://codecanyon.net/item/slider-revolution-responsive-wordpress-plugin/2751380

Packet Storm:

http://packetstormsecurity.com/files/127645/WordPress-Slider-Revolution-Responsive-4.1.4-File-Download.html

Security Focus:

http://www.securityfocus.com/bid/68942